Внешний аудит безопасности корпоративных сетей

Лекция 11
Сетевой сканер Nmap

Семён Новосёлов

2021

Crypto Kantiana

БФУ имени И. Канта

Введение

Nmap — самый популярный и продвинутый сетевой сканер.

Разработчик: Gordon Lyon

nmap.org

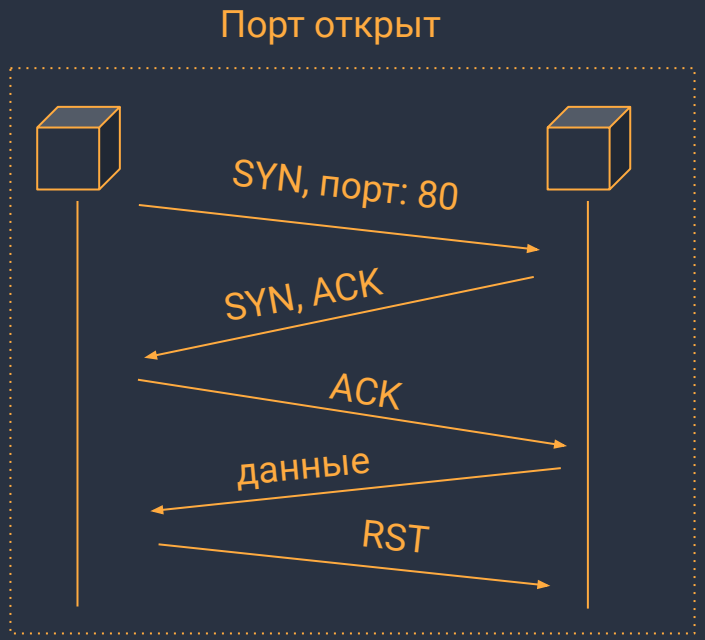
Nmap часто используется в попытках уничтожить мир

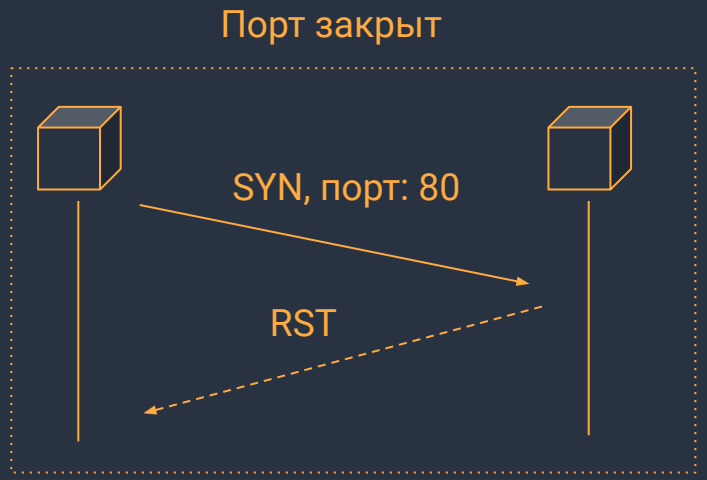
Техники сканирования портов

1. TCP-Connect
2. SYN-сканирования
3. Idle-сканирование

TCP Connect. 1/2

Принцип: попытка подключения по TCP к порту





TCP Connect. 2/2

Преимущества:

- не требует прав администратора, трудно ограничить
- может использоваться с утилитами по типу proxychains

Недостатки:

медленно, передача 5 пакетов

Пример. Сканирование через сеть TOR

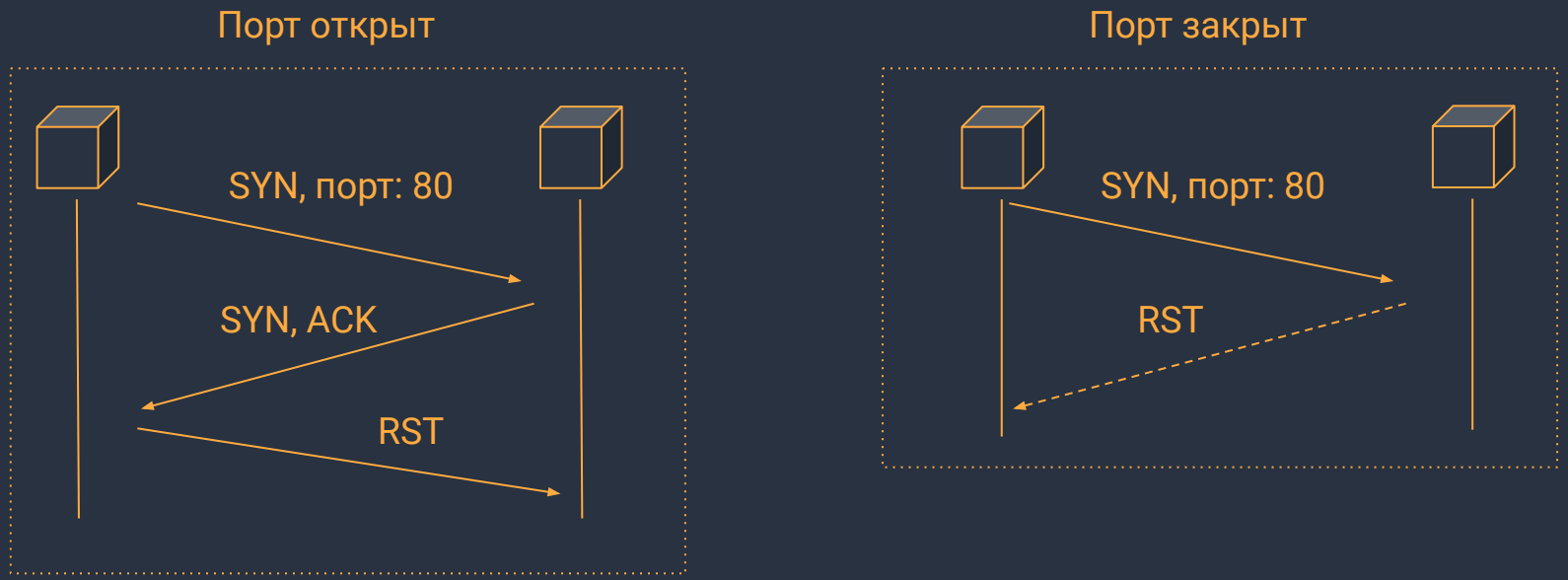

```
proxychains4 nmap -sT -PN -sV --open -n -F ya.ru
```

proxychains4 перенаправляет все TCP-соединения через цепочку прокси

Важно: протоколы ICMP/UDP/IP не затрагиваются

SYN-сканирование. 1/2

Принцип: закрывать соединение сразу же при получении SYN/ACK



SYN-сканирование. 2/2

Преимущества:

быстрое, передача 3 пакетов

Недостатки:

требует прав администратора,
через proxychains не скрывается

Idle-сканирование. 1/2

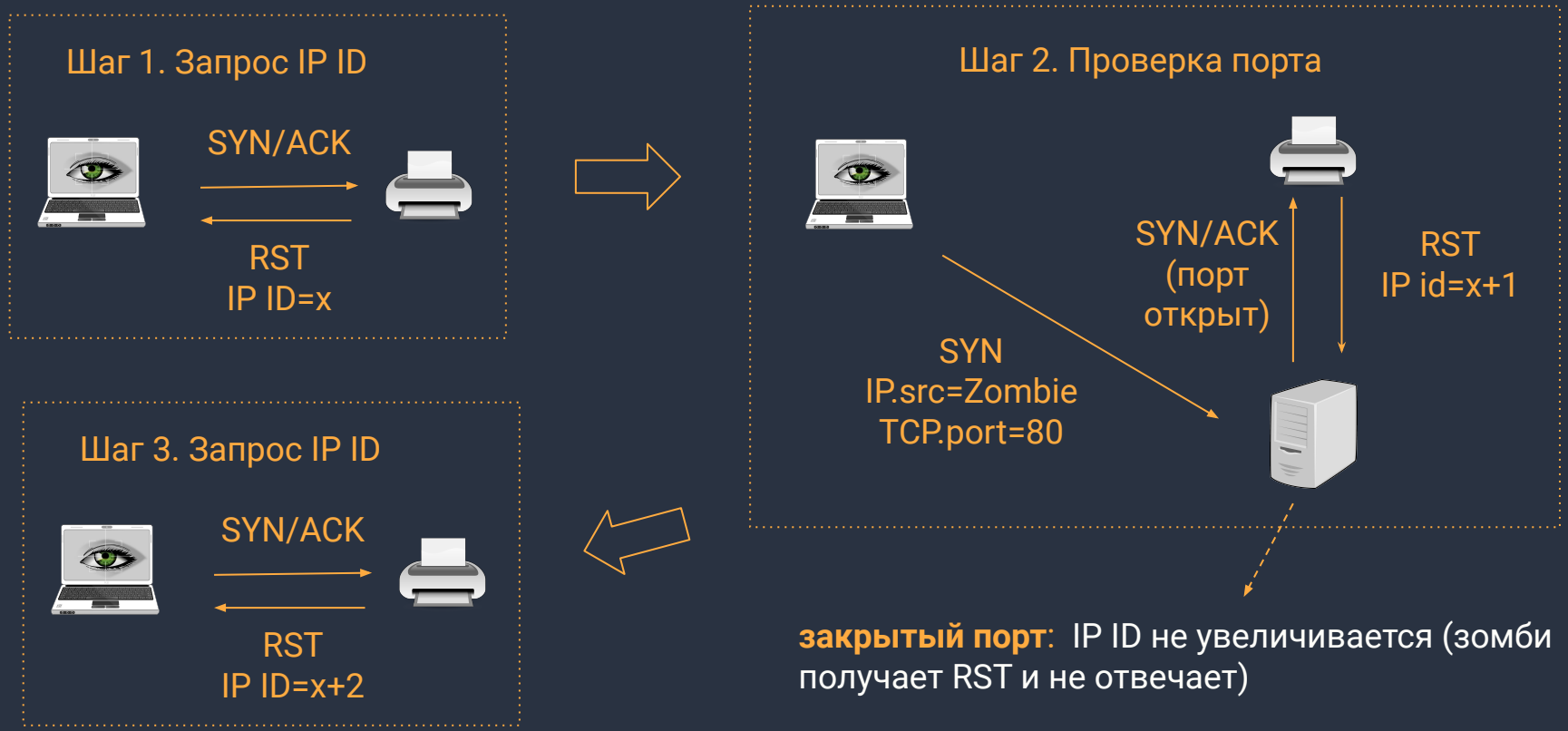
- пакеты не отсылаются на целевую машину напрямую
- скрытое сканирование через зомби-машину
- список открытых портов показывается с точки зрения зомби машины

Зомби

увеличивает IP ID на единицу при получении пакета

Поиск:
nmap --script ipidseq

Idle-сканирование. 2/2



закрытый порт: IP ID не увеличивается (зомби получает RST и не отвечает)

Определение версий сервисов

По баннеру:

текстовым строкам-идентификаторам, посылаемым сервисом

HTTP-заголовки

Server: nginx/1.16.1

Специально составленным запросам:

База **nmap-service-probes**

База запросов Nmap. Пример

```
Probe TCP GetRequest q|GET / HTTP/1.0\r\n\r\n|
ports 1,70,79,80-85, …
sslports 443
```

```
match http m|^HTTP/1\.[01] \d\d\d.*?\r\nServer: nginx\r\n|s p/nginx/ cpe:/a:igor_sysoev:nginx/
```

- `http` — сервис
- `m|^HTTP/1\.[01] \d\d\d.*?\r\nServer: nginx\r\n|s` — regex-шаблон
- `cpe:/a:igor_sysoev:nginx/` — информация о версии

Nmap Scripting Engine (NSE)

Встроенный скриптовый движок на Lua.

Список скриптов по категориям:

https://nmap.org/nsedoc/lib/nmap.html

Использование:

nmap --script http-* 192.168.1.1
nmap --script “not intrusive” 192.168.1.1

Литература и ссылки

- Gordon “Fyodor” Lyon. The Official Nmap Project Guide to Network Discovery and Security Scanning
  https://nmap.org/book/